LOS ANGELES COUNTY
INFORMATION SYSTEMS COMMISSION
383 Kenneth Hahn Hall of Administration • 500 West Temple Street • Los Angeles, CA 90012
(213) 974-1431 • (213) 633-5102 (Fax)

SUMMARY OF NOTES
of
January 12, 2009
Room 372, Kenneth Hahn Hall of Administration

Members Present
Dr. Raoul Freeman, Chair
Jonathan Fuhrman
Tom Ross
Alfred Samulon

Member Not Present
T. Austin Bordeaux
William Chen
Ying Tung Chen
Marilyn Katherman
Arnold Steinberg

Others Present
David Chittenden, Internal Services Department
Kimberly Katsuyama, EDS (Electronic Data Systems)
Robert Pittman, Chief Information Security Officer
Gary Truesdale, Hewlett-Packard Corporation
Richard Sanchez, Acting Chief Information Officer
Mike Sylvester, Department of Public Social Services

Staff
Janice Davis, Commission Services Staff

CALL TO ORDER

Chairman Freeman called the meeting to order at 3:38 p.m.

APPROVAL OF MINUTES FROM SEPTEMBER 8, 2008

Due to the lack of quorum approval of minutes was continued to the March 2, 2009 meeting.

REPORT BY CHAIRMAN AND CIO

Chairman Freeman reported Commissioner Steinberg has resigned from the Commission.

Mr. Richard Sanchez, Acting Chief Information Officer, reported the following:

- The position of the CIO is being studied and a report is being prepared to the CEO recommending a stronger alliance by the CIO with the CEO that will focus on enterprise solutions for the County.

UPDATE ON LEADER

Mr. Mike Sylvester, Assistant Director, DPSS, gave the following report:

- Four (4) major venders submitted bid proposals in May 2008.
    - Accenture
    - Deloitte
    - EDS
    - Unisys
- In October 2008 the bidders were invited to give an oral presentation of their proposals to DPSS.
- An addendum was sent out to the four (4) vendors requesting they resubmit the pricing portion of their bids by February 9, 2009, due to the economic conditions. Once the bids have been finalized the Auditor Controller will evaluate the results and the final proposals will be submitted to the Board of Supervisors in April 2009.
- On November 10, 2008 a response was received from the Legislative Analyst Office recommending the delay of Leader two (2) years because the funding was not available. On December 11, 2008, Mr. Sylvester attended a meeting with the State Department of Finance who presented reasons why delaying Leader two (2) years would cancel the project. The members of the sub-committee and the Office of Systems Integration came to a compromise with the Legislative Analyst Office and agreed to delay Leader six (6) months from January 2010 to July 2010.
- The project was included in the Governor's Budget and will be funded by the General Fund and distributed accordingly:
    - Federal 53.8%
    - State 39.9%
    - County 6.2%

OBJECTIVES FOR INFORMATION SECURITY

Mr. Robert Pittman, Chief Information Security Officer, gave the following report:

The objectives for Information Security 2009:

- Information Security Strategic Plan annual review
    - An ISSP will be emailed to Commissioners January – June 2009.
- Portable Device Initiative (3-phases)
    - Phase I – In May 2008, the County mandated that 11,000 Department laptops be encrypted with hard drives funded through Information Technology funds.
    - Phase II – The protection of USB's and CD's are sent outside of the County however the County assumes the cost. Still in process.
    - Phase III – To keep information secure a scanner searches the internet for content and data leakage both accidental and maliciously. Still being discussed.
- Countywide Security Awareness Program
    - All senior managers are required to be knowledgeable in the Security Awareness Program and that security measurements be included in all personnel evaluations.
    - The following IT security items have been implemented:
        - Smartphone Protection – Standardized security configurations
        - Laptop Protection – Full-disk encryption, secure handling guidelines and Endpoint Protection
        - Disaster Recovery – Desktop PC and laptop Protection Anti-virus
        - Internet Traffic Filtering – Browser, Web content filtering and site blocking
        - Instant Messaging – IM filtering logging
        - Network Protection – Network Firewall shield from internet
        - Web Application Protection – Server Protection
        - Server Protection – Anti-virus, host intrusion prevention, patch management, standardized security configurations
        - Countywide Information Security Program – Countywide IT security website, hotline, policies, strategy, steering committee, security engineering teams, emergency response teams
- Countywide Secure Email Project

- Legislation
    - E-Discovery
- On December 1, 2006 the Federal rules changed stating Electronically Stored Information (ESI) must have a retention record for e-mails.
    - Fair and Accurate Credit Transactions Act of 2003 “Red Flags Rules”

Legislation related to credit card information having three components.

- A policy will be developed regarding the “Red Flag Program” at the Board of Supervisors level or corporate level.
- Awareness and training of all employees in the Red Flag Program.
- Incident response and identification to a red flag.

Board of Supervisors’ Information Technology Security Policies review:

- The following policies were adopted in 2005 and sunset in July 2008. The policies are being reviewed by the CIO and will be going to the Audit Committee in February 2009.
    - 6.100 - Information Technology and Security Policy
    - 6.101 - Use of County Information Technology Resources
    - 6.102 - Countywide Antivirus Security Policy
    - 6.103 - Countywide Computer Security threat Responses
    - 6.104 - Use of Electronic Mail (e-mail) by County employees
    - 6.105 - Internet Usage Policy
    - 6.106 - Physical Security
    - 6.107 - Information Technology Risk Assessment
    - 6.108 - Auditing and Compliance

Establish Countywide Risk Management Program:

- Network Vulnerability Scanners: Scan network-connected devices for security vulnerabilities
- Application Vulnerability Scanners: Scan web-based applications for security vulnerabilities
- Database Vulnerability Scanners: Scan databases for security vulnerabilities
- Security Information and Event Management: Aggregate, correlate and analyze security events and logs; reporting and alerting

MATTERS NOT ON THE POSTED AGENDA (TO BE BRIEFLY DISCUSSED AND PLACED ON A FUTURE AGENDA)

There were none.

PUBLIC COMMENT / ANNOUNCEMENTS

There were none.

ADJOURNMENT

The meeting was adjourned at 5:00 p.m.